UNIVERSITATEA DE STAT DIN MOLDOVA

ŞCOALA DOCTORALĂ ȘTIINȚE FIZICE, MATEMATICE, ALE INFORMAȚIEI ȘI INGINEREȘTI

Cu titlu de manuscris
C.Z.U: 519.21:004.421(043.2)

MALIUTINA NADEJDA

UTILIZAREA TEHNOLOGIILOR INFORMAȚIONALE LA ELABORAREA ALGORITMILOR CRIPTOGRAFICI ȘI ALGEBRICI

Rezumatul tezei de doctor în informatică

122. 03 – Modelare, metode matematice, produse program

Autor: Maliutina Nadejda

Conducători ştiinţifici: Corlat Andrei, dr. în şt. fizico-matematice, prof. univ.

Şcerbacov Victor, dr. hab. în şt. fizico-matematice, prof. univ.

Comisia de îndrumare: Arnautov Vladimir, dr. hab. în şt. fizico-matematice, acad.

Cojocaru Svetlana, dr. hab. în informatică, m.cor., prof. cerc.

Țițchiev Inga, dr. în informatică, conf. univ.

CHIŞINĂU, 2023

Teza a fost elaborată în cadrul Școlii Doctorale Științe Fizice, Matematice, ale Informației și Inginerești, Universitatea de Stat din Moldova.

Componența Comisiei de doctorat:

Președinte:	**GAINDRIC Constantin,** doctor habilitat în informatică, profesor universitar, membru corespondent, Institutul de Matematică și Informatică "Vladimir Andrunachievici", USM;
Conducători științifici:	**CORLAT Andrei**, doctor în științe fizico-matematice, profesor universitar, Universitatea Tehnică a Moldovei; **ȘCERBACOV Victor**, doctor habilitat în științe fizico-matematice, profesor universitar, Institutul de Matematică și Informatică "Vladimir Andrunachievici", USM;
Referenți oficiali:	**CHIRIAC Liubomir,** doctor habilitat în științe fizico-matematice, profesor universitar, Universitatea Pedagogică de Stat „Ion Creangă"; **ȚIȚCHIEV Inga,** doctor în informatică, conferențiar universitar, Institutul de Matematică și Informatică "Vladimir Andrunachievici", USM; **OHRIMENCO Serghei**, doctor habilitat în economie, profesor universitar, Academia de Studii Economice; **PETIC Mircea,** doctor în informatică, conferențiar universitar, Universitatea de Stat „Alecu Russo" din Bălți;
Secretar științific:	**NOVAC Ludmila,** doctor în științe fizico-matematice, conferențiar universitar, Universitatea de Stat din Moldova.

Susținerea va avea loc la 21 aprilie 2023, orele 14:00, la Institutul de Matematică și Informatică "Vladimir Andrunachievici", str. Academiei 5, bir.340.

Teza de doctor și rezumatul pot fi consultate la Biblioteca Universității de Stat din Moldova și pe pagina web a Agenției Naționale de Asigurare a Calității în Educație și Cercetare (www.cnaa.md).

Rezumatul a fost expediat la _____ 2023.

Secretar științific al Comisiei de doctorat _____ **Novac Ludmila**

Autor _____ **Maliutina Nadejda**

CUPRINS

1. REPERELE CONCEPTUALE ALE CERCETĂRII

Actualitatea și importanța studiului

Majoritatea modelelor cunoscute de coduri de detectare și corectare a erorilor, algoritmilor criptografici și sistemelor de criptare folosesc structuri algebrice asociative, cum ar fi grupurile și câmpurile [1, 2]. Analiza studiilor a arătat că e posibil să se utilizeze astfel de structuri neasociative, ca cvazigrupurile, în multe ramuri ale teoriei codificării și mai ales în criptologie. Codurile și cifrurile bazate pe sisteme neasociative demonstrează capacități mai bune decât codurile și cifrurile cunoscute bazate pe sisteme asociative [3, 4].

Primii criptografi profesioniști, care au fost legați de dezvoltarea teoriei cvazigrupurilor au fost: A.A. Albert, A. Drisko, M.M. Glukhov, J.B. Rosser, E. Schönhardt, C.I. Mendelson și R. Schaufler. Unele rezultate, obținute în domeniul aplicării cvazigrupurilor în criptologie și teoria codificării, sunt descrise în lucrările lui J. Denes și A.D. Keedwell [3, 5-7]. Multe rezultate ale criptografiei neasociative cu cheie deschisă sunt reflectate în lucrarea lui A. Kalka [8].

Rezultate importante în aplicarea teoriei cvazigrupurilor în criptografie au fost obținute de M.E. Tuzhilin [9], Y.M. Movsisyan [10], A.V. Gribov, P.A. Zolotykh și A.V. Mikhalev [11], G. Maze, C. Monico și J. Rosenthal [12], V. Shpilrain și A. Ushakov [13], R.E. Atani, Sh.E. Atani și S. Mirzakuchaki [14], A. Krapez [15, 16], K.A. Meyer [17], V.A. Artamonov, S. Chakrabarti, V.T. Markov și S.K. Pal [18, 19].

C. Koscielny și G.L. Mullen au prezentat criptosistema cu cheie deschisă, care aplică cifruri de flux generalizate, bazate pe cvazigrupuri, în [20]. E. Ochodkova și V. Snasel [21], S. Markovski, D. Gligoroski, B. Stojcevska și V. Bakeva [22, 23], S. Markovski, V. Dimitrova, Z. Trajcheska, M. Petkovska, M. Kostadinoski și D. Buhov [24] au sugerat utilizarea cvazigrupurilor pentru codificarea sigură.

Smile Markovski și coautorii săi au prezentat un cifr de flux, bazat pe cvazigrupuri, cu o cheie aproape deschisă [22]. Algoritmul Markovski și generalizările sale în prezent sunt cunoscute pe scară largă și adesea utilizate pentru a construi cifruri de flux, bazate pe cvazigrupuri. Îmbunătățirile și cercetările algoritmului Markovski au fost intens realizate de V.A. Șcerbacov în [25].

Rezultate importante au fost obținute de A. Krapez, V. Bakeva, V. Dimitrova și A. Popovska-Mitrovikj [26-28]. A. Krapez și D. Zivkovic au propus să fie utilizate transformările parastrofice ale cvazigrupurilor și modificările acestora, care sunt foarte promițătoare pentru aplicare și cercetare [29]. Criptoanaliza acestor cifruri a fost studiată în teza lui Milan Vojvoda [30].

Unele generalizări și modificări ale algoritmului Markovski pot fi găsite în lucrările lui V.A. Șcerbacov şi A. Petrescu [31-35]. Dezvoltarea ulterioară a algoritmului Markovski este prezentată de S. Markovski, D. Gligoroski, L. Kocarev, S.J. Knapskog, M. Hassinen [36-38], C. Sucheta, K. Pal Saibal și G. Sugata [39]. Informații importante despre criptoanaliza unor cifruri de flux pot fi găsite în articolul lui V.A. Șcerbacov și P. Csorgo [40].

Algoritmul Markovski are o mulțime de diverse generalizări și poate fi utilizat pentru a construi analogi ai schemei ElGamal. Un analog al sistemului de criptare ElGamal, bazat pe algoritmul Markovski, este dat în lucrările lui V.A. Șcerbacov și N.A. Moldovyan [41], A.V. Gribov [42].

Metodele criptografice au devenit larg utilizate în comerțul electronic, telecomunicații și multe alte domenii. Aceste metode sunt folosite nu numai pentru a cripta tranzacțiile și a controla producția de criptomonede, dar și asigură funcționarea în siguranță a sistemelor bancare, a cardurilor de plastic, a ATM-urilor, a dispozitivelor fără fir etc.

Criptografia modernă se ocupă de problemele de securitate a informației, cum ar fi confidențialitatea, integritatea, autentificarea, imposibilitatea refuzului părților care dețin calitatea de autor și managementul cheilor. Crearea unor algoritmi puternici de criptare prezintă o sarcină-cheie a securității informației. Prin urmare, orice algoritm construit trebuie supus unei analize atente pentru a-i identifica punctele slabe și posibilitatea de hacking.

În teza de față sunt formulate următoarele probleme:

Problema 1. De cercetat și construit algoritmi pe baza algoritmului Markovski, folosind cvazigrupuri și grupoizi.

Problema 2. De efectuat criptoanaliza cifrurilor, care sunt construite folosind algoritmi generalizați.

Problema 1 este discutată în capitolul 2, iar problema 2 este discutată în capitolele 3 și 4.

Scopul și obiectivele tezei

Scopul cercetării științifice este de a construi algoritmi criptografici noi și de a îmbunătăți algoritmii criptografici deja construiți pe baza algoritmului Markovski, de a le realiza criptoanaliza și de a scrie programe, care implementează lucrul acestor algoritmi.

Pentru atingerea acestui scop au fost definite următoarele obiective:

- Dezvoltarea unui algoritm criptografic eficient pe baza algoritmului Markovski, folosind cvazigrupuri binare de stânga și dreapta și grupoizi n-ari;
- Dezvoltarea programelor, care implementează lucrul algoritmilor construiți;
- Efectuarea de atacuri asupra tuturor cifrurilor studiate și construite;

- Analiza comparativă a atacurilor petrecute;
- Găsirea textelor de lungime minimă pentru toate tipurile de atacuri studiate.

Ipoteza cercetării

Algoritmul clasic Markovskii poate servi ca bază pentru construirea noilor generalizări bazate pe cvazigrupuri binare și pe grupoizi care sunt inversabili într-un loc fix. Algoritmii generalizați construiți vor avea un grad mai mare de rezistență către tipurile cunoscute de atacuri. Criptoanaliza cifrurilor, construite pe baza algoritmilor generalizați, este un domeniu de studiu interesant pentru criptoanaliști.

Metode de cercetare aplicată

În această teză s-a efectuat: analiza literaturii științifice și a experienței practice, sistematizarea rezultatelor obținute anterior asupra problemei de cercetare, compararea abordărilor existente în rezolvarea problemelor, compararea metodelor moderne de construire a algoritmilor criptografici bazați pe structuri neasociative și proprietățile acestora și, în special, metode de algebră neasociativă, inclusiv metode de construire a grupoizilor n-ari, precum și metode clasice de criptoanaliză. Cercetarea se bazează pe utilizarea algoritmului clasic Markovski și generalizările acestuia.

Obiectul cercetării îl reprezintă algoritmii Markovski generalizați bazați pe cvazigrupuri binari și pe grupoizi n-ari.

Noutatea și originalitatea științifică

Toate rezultatele lucrării sunt noi și originale. Ele reprezintă o continuare a cercetărilor anterioare în acest domeniu. Au fost dezvoltați și generalizați algoritmii, care au îmbunătățit performanța algoritmului clasic Markovski, au fost construite atacuri asupra cifrurilor, folosind algoritmi generalizați și a fost arătat gradul de securitate al acestor cifruri. Rezultatele, prezentate în teză, prezintă interes pentru studiul criptologilor.

Problema științifică importantă soluționată constă în dezvoltarea unor noi modificări ale algoritmului classic, care vor ajuta la creșterea rezistenței cifrului construit la tipurile cunoscute de atacuri.

Semnificația teoretică constă în obținerea algoritmilor și cifrurilor noi îmbunătățite, folosind structuri neasociative, cum ar fi grupoizii n-ari și cvazigrupurile, în informatică. Algoritmii dezvoltați au dat posibilitate de a aborda problemele, legate cu codarea și criptoanaliza, din punct de vedere nou.

Valoarea aplicativă a tezei

Sunt propuse noi modificări ale algoritmilor de codare cu utilizarea cvazigrupurilor de stânga, cvazigrupurilor de dreapta și grupoizilor n-ari inversabili pe un loc fixat. Metodele dezvoltate au făcut posibilă rezolvarea problemelor stabilite și au conturat gama de probleme ulterioare, care nu au fost încă rezolvate. Valoarea aplicată a lucrării constă în utilizarea rezultatelor, obținute în cercetările științifice legate de codificarea datelor, în studiul eficienței prezentării informației, criptoanaliza datelor. Ele pot fi utilizate și în dezvoltarea cursurilor de specialitate pentru studenți, masteranzi și doctoranzi legate de studiul criptologiei pe structuri algebrice abstracte.

Rezultatele tezei au fost introduse în activitatea laboratorului de cercetare „Algebra și aplicațiile sale" al Universității de Stat Nistrene în numele lui T.G. Şevcenko (Tiraspol).

Publicații la tema tezei de doctorat

Rezultatele cercetării au fost publicate în 21 lucrări științifice, inclusiv 7 articole în reviste recenzate (2 articole fără coautori), 8 articole în lucrări ale conferințelor științifice (6 articole fără coautori) și 6 rezumate la conferințe științifice (2 rezumate fără coautori).

Autorul a dezvoltat direct suportul matematic și algoritmic pentru criptarea și decriptarea textelor, construite pe baza algoritmilor generalizați Markovski și, de asemenea, a efectuat o criptoanaliză a tuturor cifrurilor construite.

Structura și volumul disertaţiei

Teza constă din Introducere, patru capitole, concluzii generale și recomandări, bibliografie din 201 surse, 3 anexe, 217 de pagini (inclusiv 145 de pagini de text de bază), o figură și 71 de tabele.

Cuvinte cheie: algoritm Markovski, cvazigrup, cvazigrup de stânga și de dreapta, translație, text deschis, text cifrat, atac, cheie, criptare, descriptare.

2. CONȚINUTUL TEZEI

Structura tezei este prezentată de patru capitole, care cuprind rezultate teoretice și practice obținute în studiul și construcția generalizărilor algoritmului Markovski, precum și în criptoanaliza acestora.

Introducerea formulează actualitatea și semnificația temei de cercetare, definește obiectul cercetării, formulează scopul și obiectivele cercetării, definește metodele de cercetare, relevă noutatea științifică, semnificația teoretică și practică a disertației. Problema științifică studiată este prezentată cu accent pe importanța valorii aplicate a lucrării. Se formulează principalele prevederi depuse spre apărare, se oferă informații privind aprobarea și implementarea rezultatelor. Este prezentată o scurtă analiză a discursurilor și publicațiilor la tema tezei. La sfârșitul acestei secțiuni este un rezumat al conținutului lucrării.

Primul capitol – Situația actuală în domeniul utilizării tehnologiei informației în dezvoltarea algoritmilor criptografici și algebrici – format din șapte paragrafe, este introductiv. Oferă o imagine de ansamblu asupra stării actuale a celor mai importante domenii ale criptografiei moderne pentru munca noastră. Sunt descrise conceptele de bază ale criptologiei, necesare pentru prezentarea ulterioară a lucrării. Se face o analiză a uneia dintre cele mai utilizate clasificări ale algoritmilor criptografici și se notează ce condiții trebuie să îndeplinească algoritmii moderni de criptare.

Sunt analizate principalele caracteristici și probleme ale criptării simetrice și asimetrice. Sunt dezvăluite avantajele și dezavantajele caracteristice sistemelor moderne simetrice și asimetrice. O atenție deosebită este acordată metodelor criptoanalitice existente în prezent. Se face o trecere în revistă a utilizării structurilor algebrice neasociative în criptologie, în care atenția principală este acordată algoritmului Markovski și generalizărilor lui, construite în prezent.

În al doilea capitol – Algoritmul Markovski și noile lui generalizări – studiem funcționarea algoritmului Markovski pentru cvazigrupuri binare și caracteristicile algoritmului pentru cvazigrupurile de stânga și de dreapta. Se construiesc generalizări ale algoritmului Markovski pentru grupoizi reversibili în orice loc fixat. Acești algoritmi au fost construiți împreună cu V.A. Șcerbacov. Capitolul este format din opt paragrafe, în care s-a rezolvat obiectivul 1.

Primele trei secțiuni sunt dedicate rezultatelor obținute în studiul algoritmului Markovski în cazul aplicării cvazigrupurilor binare. Se arată că algoritmul pentru cvazigrupul stâng nu se diferă de algoritmul tradițional Markovski. Este indicată o caracteristică a algoritmului Markovski

pentru cvazigrupul drept. Au fost scrise programe, care implementează lucrul acestor algoritmi. Programele obținute lucrează pentru a cripta și decripta texte de o anumită lungime (lungimea textului poate fi schimbată cu ușurință). Programele funcționează pentru orice valori ale liderilor (liderii sunt aleși de utilizator). Cu ajutorul acestor programe se poate construi o implementare a algoritmului Markovski pentru orice cvazigrup binar.

Pe lângă cvazigrupurile binare în această construcție pot fi folosite cvazigrupurile n-are și parastrofii lor [43, 25].

Secțiunea 2.4. a tezei este dedicată construcției Algoritmului Generalizat 1.

Definim o operație n-ară f pe mulțimea Q ca $(n+1)$-tupluri de următoarea formă $\big(x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n)\big)$, unde $x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n) \in Q$.

Definiția 2.4.1. *Grupoid n-ar* (Q, f) se numește mulțimea nevidă Q cu o operație n-ară definită pe ea f.

Definiția 2.4.2. Grupoidul n-ar (Q, f) se numește *inversabil pe locul* i,unde $i = \overline{1,n}$, dacă ecuația: $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = a_{n+1}$ este rezolvabilă univoc pentru orice elemente: $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1} \in Q$ [43].

În acest caz, operația inversă ${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n) = x_i$ este definită în mod unic și avem:

$$\left.\begin{matrix} f\big(a_1, \dots, a_{i-1}, {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n\big) = a_{n+1} \\ {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = x_i \end{matrix}\right\}. \quad (\mathbf{2.1})$$

Definiția 2.4.3. *Cvazigrup n-ar* se numește groupoidul n-ar (Q, f) cu o operație n-ară f astfel încât în egalitatea $f(x_1, x_2, \dots, x_n) = x_{n+1}$ faptul cunoașterii oricăror n elemente $\{x_1, x_2, \dots, x_n, x_{n+1}\}$ definește în mod unic elementul rămas [43, 25].

Definiția 2.4.4. Grupoidul n-ar (Q, f) se numește *cvazigrup n–ar*, dacă pe mulțimea Q există operațiile ${}^{(1,n+1)}f, {}^{(2,n+1)}f, \dots, {}^{(n,n+1)}f$ astfel încât în algebra $(Q, f, {}^{(1,n+1)}f, {}^{(2,n+1)}f, \dots, {}^{(n,n+1)}f)$ pentru toți $i = \overline{1,n}$ sunt adevărate următoarele egalități:

$$\left.\begin{matrix} f\big(x_1, \dots, x_{i-1}, {}^{(i,n+1)}f(x_1, \dots, x_n), x_{i+1}, \dots, x_n\big) = x_i \\ {}^{(i,n+1)}f(x_1, \dots, x_{i-1}, f(x_1, \dots, x_n), x_{i+1}, \dots, x_n) = x_i \end{matrix}\right\}. \quad (\mathbf{2.2})$$

Este clar că numărul de grupoizi n-ari i-inversabili (numărul n este fixat) este mai mare decât numărul de cvazigrupuri n-are (numărul n este fixat). Acest fapt a servit drept imbold pentru construirea noilor generalizări ale algoritmului Markovski.

Algoritmul 2.4.5. (Algoritmul Generalizat 1). Fie Q un alfabet finit nevid și k un număr natural, $u_j, v_j \in Q, j \in \{1, \dots k\}$. Definim un grupoid n-ar (Q, f), care este inversabil pe locul i, $i = \overline{1,n}$. Atunci grupoidul $(Q, {}^{(i,n+1)}f)$ este definit în mod unic.

În acest caz, este adevărată egalitatea:

${}^{(i,n+1)}f(v_1, \dots, v_{i-1}, v_n, v_i, \dots, v_{n-1}) =$

$= {}^{(i,n+1)}f(v_1, \dots, v_{i-1}, f(v_1, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}), v_i, \dots, v_{n-1}) = u_n.$

Luăm elementele fixate $l_1^{(n-1)^2}\left(l_1, l_2, \dots l_{(n-1)^2} \in Q\right)$, pe care le vom numi lideri.

Fie $u_1, u_2, \dots u_k -$ un tuplu din k litere ale alfabetului Q.

Se sugerează următoarea procedură de criptare:

$v_1 = f(l_1, l_2, \dots, l_{i-1}, u_1, l_i, \dots, l_{n-1}),$

$v_2 = f(l_n, l_{n+1}, \dots, l_{n+i-2}, u_2, l_{n+i-1}, \dots, l_{2n-2}), \dots,$

$v_{n-1} = f\left(l_{n^2-3n+3}, \dots, l_{n^2-3n+1+i}, u_{n-1}, l_{n^2-3n+2+i}, \dots, l_{(n-1)^2}\right),$

$v_n = f(v_1, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}),$

$v_{n+1} = f(v_2, \dots, v_i, u_{n+1}, v_{i+1}, \dots, v_n),$

$v_{n+2} = f(v_3, \dots, v_{i+1}, u_{n+2}, v_{i+2}, \dots, v_{n+1}), \dots .$

Algoritmul de decriptare se construiește similar cu cazul binar și are forma:

$u_1 = {}^{(i,n+1)}f(l_1, l_2, \dots, l_{i-1}, v_1, l_i, \dots, l_{n-1}),$

$u_2 = {}^{(i,n+1)}f(l_n, l_{n+1}, \dots, l_{n+i-2}, v_2, l_{n+i-1}, \dots, l_{2n-2}), \dots,$

$u_{n-1} = {}^{(i,n+1)}f(l_{n^2-3n+3}, \dots, l_{n^2-3n+1+i}, v_{n-1}, l_{n^2-3n+2+i}, \dots, l_{(n-1)^2}),$

$u_n = {}^{(i,n+1)}f(v_1, \dots, v_{i-1}, v_n, v_i, \dots, v_{n-1}),$

$u_{n+1} = {}^{(i,n+1)}f(v_2, \dots, v_i, v_{n+1}, v_{i+1}, \dots, v_n),$

$u_{n+2} = {}^{(i,n+1)}f(v_3, \dots, v_{i+1}, v_{n+2}, v_{i+2}, \dots, v_{n+1}), \dots .$

Pentru un grupoid inversabil pe ultimul loc (caz particular, când $i = n$) algoritmul de criptare ia forma:

$v_1 = f(l_1, l_2, \dots, l_{n-1}, u_1),$

$v_2 = f(l_n, l_{n+1}, \dots, l_{2n-2}, u_2), \dots,$

$v_{n-1} = f\left(l_{n^2-3n+3}, \dots, l_{(n-1)^2}, u_{n-1}\right),$

$v_n = f(v_1, \dots, v_{n-1}, u_n),$

$v_{n+1} = f(v_2, \dots, v_n, u_{n+1}),$

$v_{n+2} = f(v_3, \dots, v_{n+1}, u_{n+2}), \dots .$

Algoritmul de decriptare în acest caz va arăta astfel:

$u_1 = {}^{(n,n+1)}f(l_1, l_2, \dots, l_{n-1}, v_1)$,

$u_2 = {}^{(n,n+1)}f(l_n, l_{n+1}, \dots, l_{2n-2}, v_2)$,…,

$u_{n-1} = {}^{(n,n+1)}f(l_{n^2-3n+3}, \dots, l_{(n-1)^2}, v_{n-1})$,

$u_n = {}^{(n,n+1)}f(v_1, \dots, v_{n-1}, v_n)$,

$u_{n+1} = {}^{(n,n+1)}f(v_2, \dots, v_n, v_{n+1})$,

$u_{n+2} = {}^{(n,n+1)}f(v_3, \dots, v_{n+1}, v_{n+2})$,… .

Lucrarea prezintă o implementare software a criptării și decriptării, utilizând Algoritmul Generalizat 1. Lungimea textului este setată la începutul programului, apoi sunt introduse valorile liderilor. Tabelul de criptare sau decriptare este introdus separat pentru fiecare caz, după ce este procesat textul simplu sau cifrat.

Remarca 2.4.9. O condiție importantă pentru funcționarea corectă a algoritmului este indicarea fără ambiguitate a valorii substituției pe locul operației inversabile.

Complexitatea algoritmului crește odată cu creșterea arității operației utilizate.

Algoritmul Generalizat 1 obținut poate fi modificat și pentru aceasta am folosit translațiile.

Secțiunea 2.5. a tezei este dedicată construirii Algoritmului Generalizat 2, folosind translații de diferit ordin.

Translația grupoidului n -ar i -inversabil (Q, f) $(n > 2)$ vom nota $T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$, unde $a_i \in Q$ pentru toți $i = \overline{1,n}$ și $T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)x = f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ pentru toți $x \in Q$.

Din definiția grupoidului n-ar i-inversabil (Q, f) urmează că orice translație a grupoidului n-ar (Q, f) este o careva permutare a elementelor din Q. Următoarea lemă va avea loc pentru orice valoare a indicelui i.

Lema 2.5.1. Dacă ${}_fT(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$ este o translație a grupoidului n-ar i-inversabil (Q, f), atunci ${}_fT^{-1}(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n) = {}_{(i,n+1)_f}T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$.

Algoritmul 2.5.2. (Algoritmul Generalizat 2). Fie Q un alfabet finit nevid și k un număr natural, $u_j, v_j \in Q, j \in \{1, \dots k\}$.

Definim grupoidul n-ar i-inversabil (Q, f), $i = \overline{1,n}$. Este clar că grupoidul $(Q, {}^{(i,n+1)}f)$ va fi definit în mod unic.

Să luăm elementele fixate: $l_1^{(n^2-n)/2}$ $\left(l_1, l_2, \dots l_{(n^2-n)/2} \in Q\right)$, pe care le numim lideri.

Fie $u_1, u_2, \dots u_k -$ un tuplu de k litere ale alfabetului Q și a, b, c, d ... numere naturale (grade ale translațiilor).

Apoi vom obține un *algoritm de criptare* de forma:

$v_1 = T^a(l_1, l_2, \dots, l_{i-2}, l_{i-1}, u_1^a, l_i, \dots, l_{n-1})$,

$v_2 = T^b(l_n, l_{n+1}, \dots, l_{n+i-3}, v_1, u_2^b, l_{n+i-2}, \dots, l_{2n-3})$,

$v_3 = T^c(l_{2n-2}, l_{2n-1}, \dots, l_{2n-i+4}, v_1, v_2, u_3^c, l_{2n-i+3}, \dots, l_{3n-6}), \dots$,

$v_{n-1} = T^d(l_{(n^2-n)/2}, v_1, \dots, v_{i-2}, u_{n-1}^d, v_{i-1}, \dots, v_{n-2})$,

$v_n = T^e(v_1, v_2, \dots, v_{i-1}, u_n^e, v_i, \dots, v_{n-1})$,

$v_{n+1} = T^f(v_2, v_3, \dots, v_i, u_{n+1}^f, v_{i+1}, \dots, v_n), \dots$.

Următoarele notații au fost utilizate în algoritm:

$u_1^a = \underbrace{f(f \dots f(l_1, l_2, \dots, l_{i-2}, l_{i-1}, u_1, l_i, \dots, l_{n-1}) \dots)}_{a\ ori}$,

$u_2^b = \underbrace{f(f \dots f(l_n, l_{n+1}, \dots, l_{n+i-3}, v_1, u_2, l_{n+i-2}, \dots, l_{2n-3}) \dots)}_{b\ ori}$,

$u_3^c = \underbrace{f(f \dots f(l_{2n-2}, l_{2n-1}, \dots, l_{2n-i+4}, v_1, v_2, u_3, l_{2n-i+3}, \dots, l_{3n-6}) \dots)}_{c\ ori}, \dots$,

$u_n^e = \underbrace{f(f \dots f(v_1, v_2, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}) \dots)}_{e\ ori}, \dots$.

Ținând cont de Lema 2.5.1. putem spune că algoritmul de decriptare poate fi construit în mod similar cu algoritmul de decriptare dat pentru Algoritmul Generalizat 1 [25].

Pentru un grupoid n-ar inversabil pe locul n, algoritmul de decriptare va avea forma:

$u_1 = (T^a)^{-1}(l_1, l_2, \dots, l_{n-1}, v_1)$,

$u_2 = (T^b)^{-1}(l_n, l_{n+1}, \dots, l_{2n-3}, v_1, v_2), \dots$,

$u_{n-1} = (T^c)^{-1}(l_{(n^2-n)/2}, v_1, \dots, v_{n-2}, v_{n-1})$,

$u_n = (T^d)^{-1}(v_1, v_2, \dots, v_{n-1}, v_n)$,

$u_{n+1} = (T^e)^{-1}(v_2, v_3, \dots, v_n, v_{n+1})$,

$u_{n+2} = (T^f)^{-1}(v_3, v_4, \dots, v_{n+1}, v_{n+2}), \dots$.

Particularitățile algoritmilor generalizați sunt ilustrate prin exemplele date în teză.

Remarca 2.5.6. O problemă importantă în Algoritmul Generalizat 2 este de a determina translațiile inverse pentru procedura de decriptare.

Lucrarea prezintă o implementare software a criptării și decriptării, utilizând Algoritmul Generalizat 2. Compararea programelor pentru doi algoritmi generalizați duce la concluzia că programele pentru al doilea algoritm sunt mult mai complicate și mai voluminoase. Complexitatea programelor depinde în primul rând de gradul translațiilor utilizate.

Dacă comparăm cei doi algoritmi construiți, vom vedea că numărul total de lideri necesari pentru primul algoritm este $(n-1)^2$, dar pentru al doilea algoritm numărul necesar de lideri este: $\frac{(n-1)n}{2}$. Al doilea număr este mai mic decât primul cu: $(n-1)\left(\frac{n}{2}-1\right)$.

Algoritmul Generalizat 2 va fi mult mai complicat, dacă pe lângă ordinul unu și doi al translației vom folosi și alte puteri. Un interes deosebit prezintă definiția translațiilor inverse pentru toate translațiile utilizate în Algoritmul Generalizat 2. Având în vedere toate aceste diferențe și caracteristici, putem concluziona că al doilea algoritm prezintă un interes mai mare pentru criptoanaliză.

Ultimele două secțiuni ale acestui capitol prezintă cercetările legate de generalizarea schemei ElGamal pe baza algoritmului Markovski.

De obicei, sistemul clasic de criptare Taher ElGamal este formulat în limbajul teoriei numerelor folosind înmulțirea după modul unui număr prim [44]. Schema ElGamal este un criptosistem cu cheie deschisă, bazat pe dificultatea de a calcula logaritmi discreți într-un câmp finit.

Pentru comoditatea unei prezentări ulterioare, amintim definiția izotopiei, pe care am folosit-o la construirea schemei generalizate ElGamal.

Definiția 2.1.6. *Operația B este izotopă operației A*, dacă $\exists\ \alpha, \beta, \gamma -$ substituții ale mulțimii Q astfel încât: $B(x,y) = \gamma^{-1}A(\alpha x, \beta y) \quad \forall x, y \in Q$, $T = (\alpha, \beta, \gamma)$ este *o izotopie*, iar α, β, γ sunt *componentele de stânga, de dreapta* și *principală* respectiv, ale acestei izotopii.

În paragraful 2.7. am considerat un analog al sistemului de criptare ElGamal pe baza algoritmului Markovski.

Fie (Q, f) un cvazigrup binar și $T = (\alpha, \beta, \gamma)$ izotopia sa.

Cheile lui Alice sunt următoarele:

Cheie deschisă: $(Q, f), T, T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k), m, n, k \in \mathbb{N}$ și algoritmul Markovski.

Cheie închisă: m, n, k.

Cheile lui Bob sunt următoarele:

Cheie deschisă: $(Q, f), T, T^{(r,s,t)} = (\alpha^r, \beta^s, \gamma^t), r, s, t \in \mathbb{N}$ și algoritmul Markovski.

Cheie închisă: r, s, t.

Criptare.

Pentru a trimite un mesaj $b \in (Q, f)$, Bob calculează $T^{(r,s,t)}$ pentru aleatoriu $r, s, t \in \mathbb{N}$.

Apoi, cunoscând $T^{(m,n,k)}$ el calculează $T^{(mr,ns,kt)}$ și $(T^{(mr,ns,kt)}(Q, f))$.

Pentru a cripta mesajul b Bob folosește algoritmul Markovski, cunoscut de Alice.

Textul cifrat este $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q,f))b)$.

Decriptare.

Alice, cunoscând m,n,k, după obținerea textului cifrat $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q,f))b)$ calculează $(T^{(mr,ns,kt)}(Q,f))^{-1}$, folosind $T^{(r,s,t)}$, și apoi calculează b.

Un exemplu de funcționare a acestei scheme este dat în lucrare.

În acest algoritm, izostrofia [45] poate fi folosită în loc de izotopie, algoritmul din [25] în loc de algoritmul Markovski și cvazigrupuri n-are ($n > 2$) [35] în loc de cvazigrupuri binare.

Următorul pas după construirea algoritmului este criptoanaliza acestuia, cu ajutorul căreia se va putea conclude despre fiabilitatea și calitatea acestuia.

Capitolul al treilea− Criptoanaliza unor cifruri de flux (cazul binar) − este format din cinci secțiuni și îndeplinește o problemă, legată de criptoanaliza cifrurilor construite în capitolul al doilea, folosind cvazigrupuri binare. Aceasta rezolvă obiectivul 2.

Pentru cvazigrupurile binare M. Vojvoda și-a desfășurat atacurile și autoarea tezei arată cum aceste rezultate pot fi îmbunătățite (pentru a efectua atacuri trunchiate), în plus, autoarea oferă atacuri modificate, care arată rezultate mai bune decât atacurile lui M. Vojvoda. Pentru fiecare caz, se stabilește numărul minim de caractere necesare pentru un atac reușit. Sunt analizate rapoartele limită ale numărului de caractere utilizate în diferite tipuri de atacuri.

M.Vojvoda a oferit criptoanaliza sistemului de codificare a fișierelor pe baza cvazigrupurilor binare [46, 30] și a arătat cum să hack acest cifr. Articolul lui M. Vojvoda [46] arată cum să hack acest cifr folosind un atac doar cu un text criptat și sunt discutate problemele de securitate ale cifrului de flux cercetat. El descrie cifrul de flux studiat, precum și generalizează rezultatele cifrului studiat la acea vreme în domeniul criptoanalizei.

În paragrafele 3.1. și 3.2. se arată cum funcționează atacurile asupra textului deschis ales și a textului cifrat pentru cvazigrupuri binare.

Mai întâi, se efectuau atacurile, folosind textul cifrat selectat.

Să presupunem că criptoanalistul are acces la dispozitivul de decriptare încărcat cu cheia. Apoi el poate construi următorul text cifrat:

$$q_1q_1q_1q_2q_1q_3 \cdots q_1q_n$$
$$q_2q_1q_2q_2q_2q_3 \cdots q_2q_n \cdots$$
$$q_nq_1q_nq_2q_nq_3 \cdots q_nq_n,$$

și să-l introducă în dispozitivul de decriptare.

Dispozitivul de decriptare oferă următorul text deschis:

$$l\backslash q_1 q_1 \backslash q_1 q_1 \backslash q_1 q_1 \backslash q_1 q_2 \backslash q_1 q_1 \backslash q_3 \cdots q_1 \backslash q_n$$
$$q_n \backslash q_2 q_2 \backslash q_1 q_1 \backslash q_2 q_2 \backslash q_2 q_2 \backslash q_2 q_2 \backslash q_3 \cdots q_2 \backslash q_n \cdots$$
$$q_n \backslash q_n q_n \backslash q_1 q_1 \backslash q_n q_n \backslash q_2 q_2 \backslash q_n q_n \backslash q_3 \cdots q_n \backslash q_n.$$

Ca urmare, tabelul Cayley al operației "\ " definite pe Q este complet găsit și construcția tabelului Cayley al operației " $*$ " este simplă. Textul cifrat folosit în atac este format din $2n^2$ caractere. Am aflat că, pentru o reconstrucție completă a tabelului Cayley pentru cvazigrupul $(Q,\backslash)$ este suficient de introdus doar $2n^2 - 4n + 1$ caractere în loc de $2n^2$. Am numit acest atac atacul trunchiat al lui M. Vojvoda.

Remarca 3.1.1. Comparând numărul de caractere, utilizate în atacul Vojvoda și atacul trunchiat Vojvoda, avem următoarea relație limitativă:

$$\lim_{n\to\infty} \frac{2n^2}{2n^2 - 4n + 1} = 1.$$

Propunem să luăm în considerare un nou tip de atac, pe care îl vom numi atac modificat. Procedura de decriptare folosește următorul text:

$$q_1 q_1 q_2 q_2 q_3 q_3 \cdots q_{n-2} q_{n-2} q_{n-1} q_{n-1} q_n q_n$$
$$q_2 q_1 q_3 q_2 q_4 q_3 \cdots q_{n-1} q_{n-2} q_n q_{n-1} q_1 q_n$$
$$q_3 q_1 q_4 q_2 q_5 q_3 \cdots q_n q_{n-2} q_1 q_{n-1} q_2 q_n \cdots .$$

Ultimul simbol depinde de paritatea ordinului cvazigrupului, și anume, dacă n este un număr impar, atunci ultima operație va fi: $q_k \backslash q_n$, unde $k = \left[\frac{n}{2}\right] + 1$. Dacă n este un număr par, atunci ultima operație va fi $q_{\frac{n}{2}} \backslash q_n$. Atacul prezentat necesită: $n^2 - 2(n-1)$ operații "\". Și ceea ce este important − acest număr nu depinde de lider.

Remarca 3.1.2. Comparând numărul de caractere utilizate în atacul Vojvoda, atacul Vojvoda trunchiat și atacul modificat, avem următoarele relații limitative:

$$\lim_{n\to\infty} \frac{2n^2}{n^2-2n+2} = 2 \text{ și } \lim_{n\to\infty} \frac{2n^2-4n+1}{n^2-2n+2} = 2.$$

Dacă comparăm acest rezultat cu rezultatul obținut în Remarca 3.1.1, vom vedea un avantaj clar al atacului modificat.

După atacurile alese cu text cifrat, am trecut la studierea atacurilor cu text ales simplu, care au propriile lor caracteristici distinctive.

Să presupunem că un criptoanalist are acces la un dispozitiv de criptare cu o cheie necunoscută. În lucrarea lui M. Vojvoda [47] următorul text este construit pentru criptare:

$$q_1q_1; q_1q_2; q_1q_3; \dots q_1q_n;$$
$$q_2q_1; q_2q_2; q_2q_3; \dots q_2q_n; \dots$$
$$q_nq_1; q_nq_2; q_nq_3; \dots q_nq_n.$$

Acest text este introdus în dispozitivul de criptare discret câte 2 caractere. Datorită acestei introduceri, avem următorul text cifrat:

$$l * q_1 \ \ (l * q_1) * q_1; l * q_1 \ \ (l * q_1) * q_2; \dots l * q_1 \ \ (l * q_1) * q_n;$$
$$l * q_2 \ \ (l * q_2) * q_1; l * q_2 \ \ (l * q_2) * q_2; \dots l * q_2 \ \ (l * q_2) * q_n; \dots$$
$$l * q_n \ \ (l * q_n) * q_1; l * q_n \ \ (l * q_n) * q_2; \dots l * q_n \ \ (l * q_n) * q_n.$$

Textul simplu utilizat în atac este format din $2n^2$ caractere împărțite în perechi. Cu toate acestea, se poate construi un text criptat mai scurt format din $2(n-1)^2$ caractere (atacul lui M. Vojvoda trunchiat).

Ieșirea, adică linie cu linie într-o poziție impară, este numărul liniei, iar la o poziție pară – este elementul cvazigrupului $(Q, *)$. Avantajul acestor atacuri este că nu depind de liderul folosit.

Acum precăutăm opțiunea, când caracterele sunt lansate în dispozitivul de criptare printr-un flux, și anume, ca în cazul unui atac cu un text cifrat selectat:

$$q_1 \ q_1 \ q_1 \ q_2 \ q_1 \ q_3 \dots q_1 \ q_n$$
$$q_2 \ q_1 \ q_2 \ q_2 \ q_2 \ q_3 \dots q_2 \ q_n \dots$$
$$q_nq_1 \ q_nq_2 \ q_nq_3 \dots q_nq_n \dots .$$

Am numit acest atac atacul de streaming Vojvoda. În acest atac, numărul de simboluri folosite este mai mic decât în cele două atacuri anterioare, dar rezultatul depinde de lider. Acesta este dezavantajul atacului de streaming.

Pentru fiecare caz, puteți alege un atac de streaming cu un număr minim de caractere, dar această sarcină este destul de dificilă. Pentru un cvazigrup de ordinul n, numărul minim necesar de simboluri este: $n(n-2)+2$.

Acum cercetăm un atac modificat, folosind text simplu selectat cu introducere de caractere discrete:

$$q_1q_1; q_2q_2; q_3q_3; \dots q_{n-2}q_{n-2}; q_{n-1}q_{n-1}; q_nq_n;$$
$$q_2q_1; q_3q_2; q_4q_3; \dots q_{n-1}q_{n-2}; q_nq_{n-1}\ ; q_1q_n;$$
$$q_3q_1; q_4q_2; q_5q_3; \dots q_nq_{n-2}; q_1q_{n-1}; q_2q_n \dots .$$

Textul deschis folosit în acest atac este format din $2(n-1)^2$ caractere împărțite în perechi. Rezultatul atacului modificat a coincis cu rezultatul atacului trunchiat al lui M. Vojvoda. Astfel, chiar și în cazul binar, atunci când se efectuează atacuri cu un text cifrat ales sau cu text deschis ales, numărul simbolurilor utilizate poate fi redus.

Am luat în considerare modificările criptoatacurilor, construite de M. Vojvoda pentru cvazigrupuri, am efectuat analiza comparativă și am identificat părți pozitive și negative în aceste atacuri.

În secțiunile 3.3. și 3.4. sunt arătate cum funcționează atacurile asupra textului deschis și asupra textului cifrat ales pentru cvazigrupurile de stânga și de dreapta.

În primul rând, au fost luate în considerare atacurile efectuate folosind textul cifrat ales. Vă prezentăm rezultatele acestor atacuri.

Pentru o reconstrucție completă a tabelului Cayley pentru cvazigrupul de stânga $(Q, \setminus)$, este suficient de introdus doar $2n^2 - 2n + 1$ caractere la intrare în loc de $2n^2$. Acesta este un atac trunchiat.

Am oferit un atac modificat. Dacă rulăm următorul text pe decodor:

$$q_1q_1q_2q_2q_3q_3 \cdots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3 \cdots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3 \cdots q_nq_{n-2}q_1q_{n-1}q_2q_n \cdots,$$

ultimul simbol depinde de paritatea ordinului cvazigrupului, și anume, dacă n este un număr impar, atunci ultima operație va fi: $q_n \setminus q_k$, unde $k = \left[\frac{n}{2}\right] + 1$. Dacă n este un număr par, atunci ultima operație va fi: $q_n \setminus q_{\frac{n}{2}+1}$.

Atacul prezentat necesită: $n^2 - 2\left(n - 1 - \left[\frac{n}{2}\right]\right)$ operații " \". În comparație cu atacul lui M. Vojvoda, numărul simbolurilor folosite este semnificativ redus.

În continuare, am luat în considerare atacurile cu text deschis ales pentru cvazigrupurile de stânga. Textul deschis folosit în atacul lui M. Vojvoda constă din $2n^2$ caractere împărțite în perechi. Cu toate acestea, poate fi construit un text mai scurt format din $2n^2 - 2n$ caractere. În cazul introducerii de caractere discrete, rezultatele atacului trunchiat și ale atacului modificat sunt aceleași. Când se ia în considerare un atac de streaming cu text deschis ales, rezultatul depinde de liderul utilizat.

Cel mai bun rezultat este obținut la utilizarea unui atac de streaming modificat. În acest atac, numărul de caractere folosit este $(n-1)n + 1$, unde $n -$ este ordinea cvazigrupului de stânga folosit pentru criptare.

Rezultatele obținute din atacurile cu text cifr ales și text deschis ales asupra cifrului Markovski generalizat bazat pe cvazigrupuri de dreapta sunt similare cu cele cu cvazigrupuri de stânga.

Aplicarea tuturor atacurilor date este ilustrată printr-un șir de exemple.

Capitolul al patrulea – Criptanaliza unor cifruri de flux (caz n-ar) – format din trei paragrafe, rezolvă problema legată de criptoanaliza cifrurilor, construite cu ajutorul algoritmului Markovski generalizat bazat pe grupoizi n-ari i-reversibili, și anume Algoritmul Generalizat 1. Aceasta rezolvă obiectivul 2.

În secțiunea 4.1 au fost investigate atacuri cu un text cifru ales construit pe baza grupoidului n-ar i-inversabil, folosind Algoritmul Generalizat 1. Sunt prezentate modificări ale acestor atacuri. S-a găsit numărul necesar de caractere pentru a efectua cu succes un atac cu textul cifrat ales. Pentru o serie de cazuri, sunt oferite exemple de texte cu lungime minimală. Din toate atacurile și cercetările efectuate se trag concluzii. Să aruncăm o privire asupra celor mai importante dintre ele.

Să presupunem că criptoanalistul are acces la dispozitivul de decriptare încărcat cu cheia. Apoi poate construi următorul text cifrat, unde n este aritatea și m este ordinul unui grupoid i-inversabil:

$$\underbrace{q_1q_1\cdots q_1q_1}_{n\ ori}\underbrace{q_1q_1\cdots q_1q_2}\cdots\underbrace{q_1q_m\cdots q_mq_m}$$

$$\underbrace{q_2q_1\cdots q_1q_1}\underbrace{q_2q_1\cdots q_1q_2}\cdots\underbrace{q_2q_m\cdots q_mq_m}$$

$$\underbrace{q_3q_1\cdots q_1q_1}\underbrace{q_3q_1\cdots q_1q_2}\cdots\underbrace{q_3q_m\cdots q_mq_m}\cdots,$$

și îl introduce în dispozitivul de decriptare.

Acest text este o versiune generalizată a textului folosit de M. Vojvoda pentru cvazigrupuri binare.

Pentru o reconstrucție completă a tabelului de valori al operației ${}^{(i,n+1)}f$, și deci a tabelului de valori al operației f, este suficient să se prezinte la intrare: $(n\cdot m^{n-1}+1)(m-1)$ caractere pentru a obține toate valorile.

S-a determinat lungimea textului minim necesar și s-au construit astfel de texte pentru unele cazuri. De exemplu, pentru cazul $n=m=3$ avem nevoie de 56 de caractere pentru a restabili complet tabelul cu valorile funcției ${}^{(i,4)}f$.

Am îmbunătățit acest rezultat și am propus următorul text pentru a fi introdus în dispozitivul de decriptare:

$q_1q_1q_1q_2q_2q_2q_3q_3q_3$		000111222
$q_2q_1q_1q_3q_2q_2\ q_1q_3q_3$	sau	100211022
$q_1q_2q_1q_2q_3q_2q_3q_1q_3$		010121202
q_1q_1		00.

La ieșire s-au primit 29 caractere, ceea ce este suficient pentru a restabili complet toate valorile funcției ${}^{(i,4)}f$.

Deci numărul minim de caractere într-un atac modificat va fi: $m^n + (n-1)$.

În urma acestor două atacuri, reușim să restabilim toate valorile funcției de decriptare. Principala problemă a atacului modificat este selectarea textelor optime pentru grupoizi de diferit grad și ordin.

Este de remarcat că pentru valorile funcției f și ale funcției ei inverse ${}^{(i,n+1)}f$ pe următoarele mulțimi: $(q_{j_1}, q_{j_2}, \dots q_{j_{i-1}}, q_i, q_{j_{i+1}}, \dots q_{j_n})$, unde elementele $q_{j_1}, q_{j_2}, \dots q_{j_{i-1}}, q_{j_{i+1}}, \dots q_{j_n}$ sunt alese din mulțimea $\{q_1, q_2, \dots q_m\}$ și sunt elemente fixate, pentru diferite valori ale elementului q_i – funcțiile corespunzătoare nu pot lua aceleași valori. Deci, pentru fiecare astfel de set fixat, este suficient de determinat $m-1$ valori ale funcției corespunzătoare, iar apoi ultima valoare va fi găsită automat. Ținând cont de această remarcă, textul construit va avea lungimea: $m^{n-1} \cdot (m-1)$.

Cu toate acestea, există două caracteristici ale acestui text care trebuie remarcate:

1) Determinarea valorilor funcțiilor rămase (au rămas m^{n-1}) este o sarcină mai dificilă decât în cazul lucrului cu cvazigrupuri binare;

2) Pentru cazul $n = m = 3$, am selectat un astfel de text, însă e posibil să selectăm text similar în alte cazuri? Și va fi posibil să găsim forma generală a unui astfel de text, sau va fi diferit pentru fiecare caz?

De exemplu, pentru cazul $n = m = 3$, pentru a restabili tabelul de valori al operației ${}^{(i,4)}f$, este suficient să introducem 20 de caractere (vom restabili 18 valori din 27):

$$q_1q_1q_1q_2q_2q_2q_3q_3q_3 \quad 000111222$$
$$q_2q_1q_2q_1q_3q_1q_3q_2q_3 \quad \text{sau} \quad 101020212$$
$$q_1q_2 \quad 01.$$

Acest text are cea mai mică lungime pentru cazul $n = m = 3$. O caracteristică a acestui atac este că nu obținem toate valorile funcției, ci doar un număr suficient de caractere pentru a restabili întregul tabel.

Să presupunem că acum cheia este hack și trebuie să hack textul decriptat. Situația va fi următoarea: primele $(n-1)$ simboluri, care conțin lideri, pot lua orice valoare, iar toate celelalte simboluri vor fi determinate de acestea. Prin urmare, posibilele opțiuni ale textelor descifrate vor fi: m^n.

În secțiunea 4.2. am considerat atacurile cu textul deschis ales, construit cu aplicarea grupoizilor n-ari i-inversabili, obținut cu ajutorul Algoritmului Generalizat 1. O caracteristică a unor astfel de atacuri este că e imposibil de ales versiunea optimă a textului general pentru ei.

Să presupunem că criptoanalistul are acces la dispozitivul de criptare încărcat cu cheia. El poate construi următorul text deschis (n este aritatea operației și m este ordinul grupoidului i-inversabil):

$$\underbrace{q_1q_1 \cdots q_1q_1}_{n\ ori}\ \underbrace{q_1q_1 \cdots q_1q_2} \cdots \underbrace{q_1q_1 \cdots q_1q_m}$$

$$\underbrace{q_1q_1 \cdots q_2q_1}\ \underbrace{q_1q_1 \cdots q_2q_2} \cdots \underbrace{q_1q_1 \cdots q_2q_m}$$

$$\underbrace{q_1q_1 \cdots q_3q_1}\ \underbrace{q_1q_1 \cdots q_3q_2} \cdots \underbrace{q_1q_1 \cdots q_3q_m} \cdots$$

$$\underbrace{q_1q_1 \cdots q_mq_1}\ \underbrace{q_1q_1 \cdots q_mq_2} \cdots \underbrace{q_1q_1 \cdots q_mq_m} \cdots,$$

și îl introduce în dispozitivul de criptare.

Numărul de caractere necesare pentru a restabili tabelul de criptare depinde de valorile liderilor selectați. Prin urmare, problema determinării lungimii textului deschis utilizat în fiecare caz este decisă individual. Lucrarea acestui tip de atac este ilustrată printr-o serie de exemple.

În concluzie, aș vrea să spun câteva cuvinte despre criptoanaliza cifrurilor construite pe baza Algoritmului Generalizat 2. Această criptoanaliză este o problemă foarte dificilă, din cauza faptului că nu cunoaștem gradul translațiilor folosite în algoritm. Acest lucru indică din nou că Algoritmul Generalizat 2 este mai rezistent la criptoanaliză decât Algoritmul Generalizat 1.

Având în vedere cercetările efectuate, putem conclude că ambii algoritmi generalizați prezintă un mare interes pentru utilizarea în criptografie.

3. CONCLUZII GENERALE ȘI RECOMANDĂRI

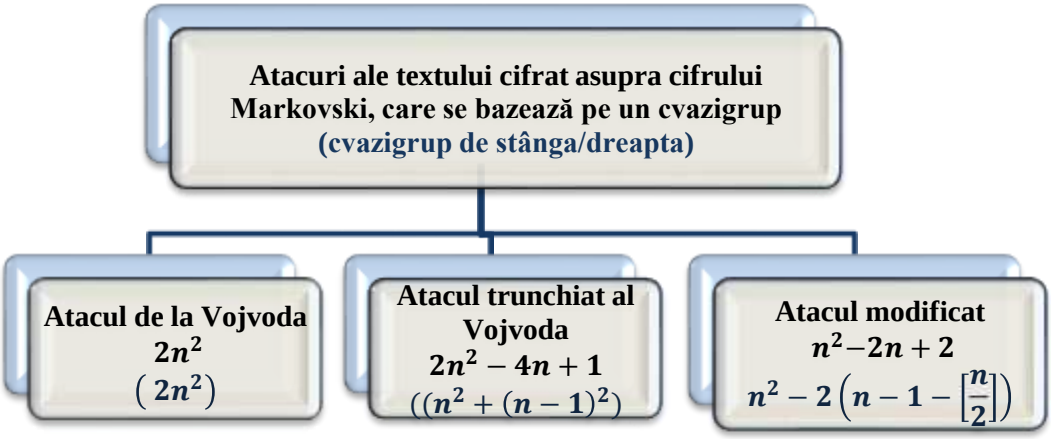
Cercetările efectuate în cadrul tezei de doctorat „**Utilizarea tehnologiilor informaționale în dezvoltarea algoritmilor criptografici și algebrici**” corespunde pe deplin scopului și obiectivelor expuse în capitolul introductiv.

Rezultatele principale ale lucrării sunt noi și originale. S-au dezvoltat și generalizat algoritmi care au îmbunătățit lucrul algoritmului clasic Markovski; au fost studiate atacurile asupra cifrurilor construite și s-a arătat gradul de rezistență al acestor cifruri.

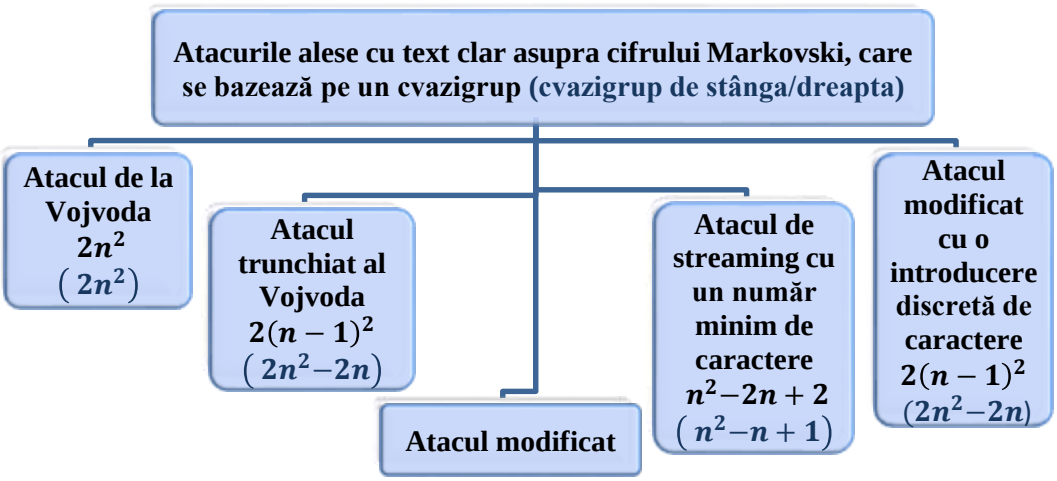
Semnificația teoretică a tezei este determinată de obținerea algoritmilor și cifrurilor noi construite, aplicând structurile neasociative, cum ar fi grupoizii n-ari și cvazigrupurile. Valoarea aplicativă a tezei constă în utilizarea rezultatelor obținute în teoria codificării și criptoanaliză.

Analiza rezultatelor obținute ne permite să evidențiem următoarele rezultate generale:

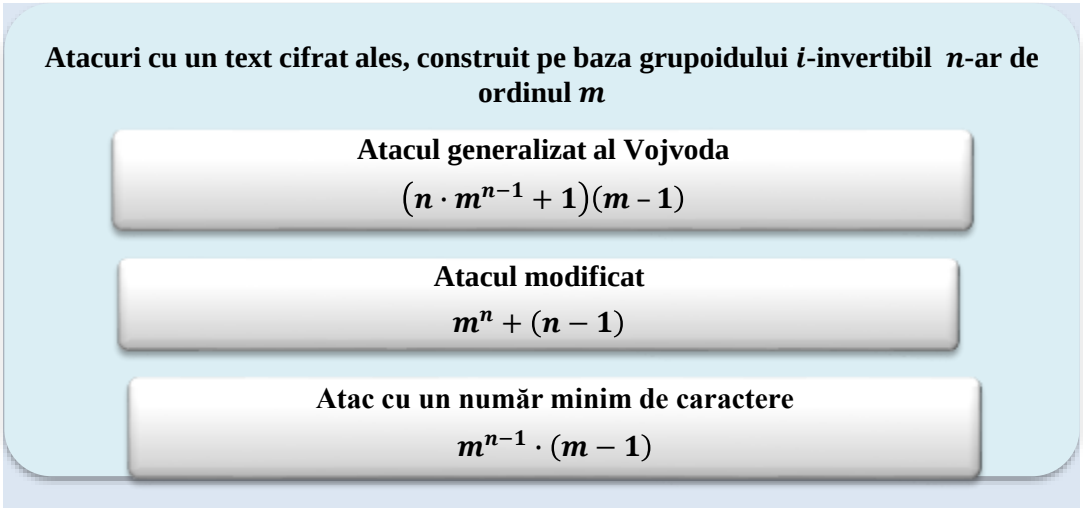
1. Sarcina cheie a protecției informațiilor este de a crea algoritmi de criptare puternici, astfel încât orice algoritm nou construit trebuie supus unei analize atente pentru a-i identifica punctele slabe și posibilitatea de rupere.
2. Utilizarea cvazigrupurilor în criptologie arată posibilități și rezultate mai bune decât utilizarea sistemelor asociative.
3. S-au dezvoltat algoritmi Markovski generalizați pentru cvazigrupuri de stânga și de dreapta și programe pentru implementarea lor (Anexa 2), iar acești algoritmi au propriile caracteristici și avantaje.
4. Atacuri ale textului cifrat ales au fost efectuate pe cifrurile Markovski, construite folosind cvazigrupurile (cvazigrupurile de stânga și cvazigrupurile de dreapta); s-a efectuat o analiză comparativă; s-au identificat aspecte pozitive și negative ale acestor atacuri și s-au propus atacuri noi modificate cu rezultate îmbunătățite.



5. Atacuri ale textului deschis au fost efectuate pe cifrurile Markovski, construite folosind cvazigrupurile; s-au identificat aspecte pozitive și negative ale acestor atacuri și s-au propus atacuri noi modificate cu rezultate îmbunătățite. Pentru atacurile de streaming cu ajutorul textului simplu selectat, se determină numărul minim de caractere necesare pentru a restabili complet tabelul cvazigrupului de criptare (textul depinde de liderul folosit).

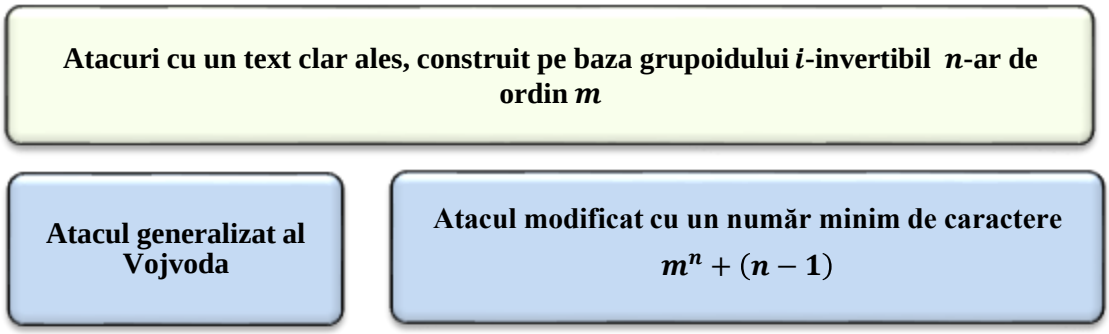


6. S-a construit un algoritm Markovski generalizat pentru un grupoid n-ar inversabil pe un loc fixat - Algoritmul Generalizat 1 și au fost scrise programe care implementează lucrul acestui algoritm.
7. Atacurile au fost descrise folosind textul cifrat ales asupra unui cifru obținut prin utilizarea algoritmului generalizat Markovski (Algoritmul Generalizat 1).



8. Un atac asupra textului cifrat poate fi efectuat prin enumerarea exhaustivă a tuturor valorilor funcțiilor în care apar lideri. Numărul total al acestor valori este m^{n-1}.

9. Atacurile au fost descrise folosind textul deschis ales asupra unui cifru obținut prin utilizarea algoritmului generalizat Markovski (Algoritmul Generalizat 1).



10. Pentru groupoid de ordinul al treilea și al patrulea au fost construite texte de cea mai scurtă lungime, dar în fiecare caz sunt selectate individual. Selectarea unui astfel de text este o sarcină dificilă pentru atacurile de text deschis ales.
11. A fost construit un algoritm Markovski generalizat pentru un grupoid n-ar inversabil pe un loc fixat, folosind translații de orice grad - Algoritmul Generalizat 2 și au fost elaborate programe care implementează lucrul acestui algoritm.
12. Numărul total de lideri necesari pentru primul algoritm va fi: $(n-1)^2$, iar pentru al doilea algoritm numărul necesar de lideri va fi egal cu: $\frac{(n-1)n}{2}$. Al doilea număr este mai mic decât primul cu valoarea: $(n-1)\left(\frac{n}{2}-1\right)$. Asta sugerează avantajul celui de-al doilea algoritm față de primul (în special cu creșterea numărului n).
13. Algoritmul Generalizat 2 va fi mult mai complicat dacă pe lângă gradul 1 și 2 al translațiilor vom folosi al treilea, al patrulea și alte grade superioare ale translațiilor. De un interes deosebit este determinarea translațiilor inverse, care sunt aplicate în Algoritmul Generalizat 2.
14. A fost efectuată o analiză a tuturor programelor dezvoltate, care include o evaluare a celor mai importanți parametri (printre aceștia: lungimea textului, algoritmul utilizat, numărul de elemente de lider necesare, viteza medie de procesare a datelor și estimarea complexității algoritmului folosind conceptul Big-O). Ca urmare, sa concluzionat că programele funcționează cu succes și au caracteristici pozitive.
15. Am considerat un analog al sistemului de criptare ElGamal bazat pe algoritmul Markovski și au fost studiate caracteristicile acestuia. Pentru acesta sunt planificate noi modificări. Criptoanaliza acestei scheme generalizate este o problemă complexă, care trebuie rezolvată.

Elaborarile propuse au o valoare științifică semnificativă datorită gradului lor înalt de noutate si originalitate. Rezultatele obținute în această teză au o valoare teoretică şi aplicativă în domenii precum algebra, criptologia și informatica.

Recomandări:

1. Un interes deosebit este aplicarea ulterioară a algoritmului Markovski în teoria codificării și mai ales în criptografie;
2. Cercetările pe tema tezei pot fi continuate atât din punct de vedere algebric, cât și aplicativ. De interes deosebit este studiul posibilităților de utilizare a cvazigrupurilor și a altor sisteme neasociative în criptologie și teoria codificării;
3. Algoritmii construiți pot fi utilizați în sistemele informaționale bancare, precum și în dezvoltarea diferitelor produse bancare, ca protecție suplimentară care crește fiabilitatea și durabilitatea acestor sisteme și produse (de exemplu, în cardurile moderne din plastic).
4. Rezultatele obţinute pot fi folosite pentru a dezvolta algoritmi algebrici şi criptografici în diverse domenii ale informaticii;
5. Conținutul tezei poate servi drept bază pentru dezvoltarea unor cursuri speciale pentru doctoranzi și masteranzi.

BIBLIOGRAFIE

[1] MAGLIVERAS, STINSON and VAN TRUNG, T. New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups. In: *J. Cryptology*, 2002, vol.15, no.4, pp. 285-297. ISSN 1432-1378.

[2] DEHORNOY, P. Braid-based cryptography. In: *Contemporary Mathematics, Group Theory, Statistics, and Cryptography*, 2004, vol. 360, pp. 5-33. ISBN 978-0-8218-3444-2.

[3] DENES, J. and KEEDWELL, A. D. Some applications of non-associative algebraic systems in cryptology. In: *Pure Mathematics and Applications*., 2001, vol. 12(2), pp.147-195. ISSN 1218-4586.

[4] KOSCIELNY, Cz. $NLPN$ Sequences over $GF(q)$. In: *Quasigroups and Related Systems*, 1997, vol.4, no.1, pp. 89-102. ISSN 1561-2848.

[5] DENES, J. and KEEDWELL, A. D. Latin Squares and their Applications. In: *Bulletin of the American mathematical society*, May 1976, Vol.82, No.3, pp. 468-471. ISSN 0273-0979.

[6] DENES, J. and KEEDWELL, A.D. Latin squares: New Developments in the Theory and Applications. In: *Annals of Discrete mathematics*, 1991, North-Holland, vol. 46, pp. 1-469. ISSN 0167-5060. ISBN 0 444 88899 3.

[7] DENES, J. On Latin squares and a digital encrypting communication system. In: *P.U.M.A., Pure Mathematics and Applications*, Department of Mathematics, Corvinus University of Budapest, 2000, vol. 11, iss.4, pp.559-563. ISSN 1218-4586.

[8] KALKA, A. *Non-associative public-key cryptography*, 2012, 32 p. [Online]. Disponibil: https://arxiv.org/pdf/1210.8270.pdf

[9] ТУЖИЛИН, М. Э. Латинские квадраты и их применение в криптографии. В: *Прикладная дискретная математика, Математические методы криптографии*, 2012, №3(17), стр. 47-52. ISSN 2311-2263 (Online).

[10] МОВСИСЯН, Ю. Сверхтождества в алгебрах и многообразиях. В: *Успехи математических наук*, 1998, том 53, выпуск 1(319), стр. 61-114. ISSN 0042-1316.

[11] ГРИБОВ, А.В., ЗОЛОТЫХ, П.А., МИХАЛЕВ, А.В. Построение алгебраической криптосистемы над квазигрупповым кольцом. В: *Математические вопросы криптографии*, 2010, том 1, выпуск 4, стр. 23-32. ISSN 2220-2617.

[12] MAZE, G., MONICO, C. and ROSENTHAL, J. Public key cryptography based on semigroup actions. In: *Advances in Mathematics of Communications*, 2007, Vol.1, No.4, pp.489-507. ISSN 1930-5346.

[13] SHPILRAIN, V. and USHAKOV, A. Thompson's Group and Public Key Cryptography. In: *Applied Cryptography and Network Security*. ACNS 2005. Lecture Notes in Computer Science, Springer, vol. 3531, pp.151-163. ISBN 978-3-540-26223-7. ISSN 0302-9743.

[14] ATANI, R.E., ATANI, SH.E. and MIRZAKUCHAKI, S. Public Key Cryptography Based on Semimodules over Quotient Semirings. In: *International Mathematical Forum*, 2007, Vol.2, No.52, pp.2561-2570. ISSN 1312-7594.

[15] KRAPEZ, A. Cryptographically Suitable Quasigroups via Functional Equations. In: *ICT Innovations 2012*, Advances in Intelligent Systems and Computing, 2013, vol. 207, pp. 265-274. ISSN 1857-7288.

[16] KRAPEZ, A. ŠEŠELJA, B., TEPAVČEVIĆ, A. Solving linear equations by fuzzy quasigroups techniques. In: *Information Sciences*. 2019, vol. 491, pp.179-189. ISSN 0020-0255.

[17] MEYER, K. A. *A New Message Authentication Code Based on the Non-Associativity of Quasigroups*. PhD thesis of doctor of philosophy, Iowa State University, 2006, 91 p.

[18] ARTAMONOV, V. Applications of quasigroups to cryprography. In: *Sarajevo Journal of Mathematics.* 2018, vol.14 (27), no.2, pp. 191–205. ISSN 1840-0655.

[19] ARTAMONOV, V., CHAKRABARTI, S., MARKOV, V., PAL, S. Constructions of polynomially complete quasigroups of arbitrary order. In: *Journal of Algebra and Its Applications.* 2020, vol.20, no.12, 2150236. ISSN 0219-4988.

[20] KOSCIELNY, Cz. and MULLEN, G.L. A quasigroup-based public-key cryptosystem. In: *International Journal of Applied Mathematics and Computer Science*, 1999, Vol.9, No.4, pp. 955-963. ISSN 1641-876X.

[21] OCHODKOVA, E. and SNASEL, V. Using quasigroups for secure encoding of file system. In: *Proceedings of the Conference Security and Protection of Information*, Abstract of Talks, Military Academy in Brno, 2001, pp. 175-181. ISBN 8085960281.

[22] MARKOVSKI, S., GLIGOROSKI, D. and STOJCEVSKA, B. Secure two-way on-line communication by using quasigroup enciphering with almost public key. In: *Novi Sad Journal of Mathematics*, 2000, Vol. 30, Iss.2, pp. 43-49. ISSN 0352-0900.

[23] MARKOVSKI, S., GLIGOROSKI, D. and BAKEVA, V. Quasigroup string processing: Part 1. In: *Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci*. XX (1-2), 1999, pp.13-28. ISSN 1857-9027.

[24] MARKOVSKI, S., DIMITROVA, V., TRAJCHESKA, Z., PETKOVSKA, M., KOSTADINOSKI, M., BUHOV, D. Block cipher defined by matrix presentation of quasigroups. In: *IACR Cryptology ePrint Archive*. 2021, vol. 2021/ 1512, 3 p.

[25] SHCHERBACOV, V.A. *Elements of Quasigroup Theory and Applications*. (1st ed.). Chapman and Hall/CRC, 2017, 598 p. ISBN 9781315120058.

[26] BAKEVA, V. and DIMITROVA, V. Some probabilistic properties of quasigroup processed strings useful in cryptanalysis. In: *Communications in Computer and Information Science*, 2011, Vol.83, pp. 61-70. ISSN 1865-0929.

[27] BAKEVA, V., DIMITROVA, V. and POPOVSKA-MITROVIKJ, A. Parastrophic quasigroup string processing. In: *Proceedings of the 8th Conference on Informatics and Information Technologies with International Participation*, 2011, Bitola, Macedonia, pp.19-21.

[28] DIMITROVA, V., BAKEVA, V., POPOVSKA-MITROVIKJ, A. and KRAPEZ, A. Classifications of quasigroups of order 4 by parastrophic quasigroups tranformation. In: *The International Mathematical Conference on Quasigroups and Loops, LOOPS'11*, Booklet of Abstracts, Trest, Czech Republic, 2011, p.6.

[29] KRAPEZ, A. and ZIVKOVIC, D. Parastrophically equivalent quasigroup equations. In: *Publications de l'Institut Mathématique*, Nouvelle Série, Beograd, 2010, Vol.87(101), pp.39-58. ISSN 0350-1302.

[30] VOJVODA, M. *Stream Ciphers and Hash Functions: Analysis of Some New Design Approaches*: PhD thesis in technical sciences. Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Bratislava, Slovak Republic, 2004. 94 p

[31] SHCHERBACOV, V.A., *Elements of quasigroup theory and some its applications in code theory and cryptology*, 2003, 85 p. [online]. Disponibil: https://www2.karlin.mff.cuni.cz/~drapal/speccurs.pdf

[32] SHCHERBACOV, V.A. *On some known possible applications of quasigroups in cryptology*, 2003, 15 p. [online]. Disponibil: https://www2.karlin.mff.cuni.cz/~drapal/krypto.pdf

[33] PETRESCU, A. Applications of quasigroups in cryptography. In: *Interdisciplinarity in Engineering Scientific International Conference Tg. Mures*-Romania, 15-16 November, 2007, 5 p. ISSN 2285-0945.

[34] PETRESCU, A. n -Quasigroup cryptographic primitives: Stream ciphers. In: *Studia Universitatis Babeș-Bolyai Informatica*, 2010, Vol. LV, Iss.2, pp. 27-34. ISSN 1224-869X.

[35] SHCHERBACOV, V.A. Quasigroups in cryptology. In: *Computer Science Journal of Moldova*, 2009, vol.17, no.2(50), pp. 193-228. ISSN 1561-4042.

[36] GLIGOROSKI, D., MARKOVSKI, S. and KOCAREV, L. Edon-R, an infinite family of cryptographic hash functions. In: *International Journal of Network Security*, 2009, Vol.8, No.3, pp.293-300. ISSN 1816-353X.

[37] GLIGOROSKI, D., MARKOVSKI, S. and KNAPSKOG, S. J. *A public key block cipher based on multivariate quadratic quasigroups*, 2008, 22 p. [Online]. https://arxiv.org/abs/0808.0247

[38] HASSINEN, M. and MARKOVSKI, S. Secure SMS messaging using Quasigroup encryption and Java SMS API. In: *Proceedings of the Eighth Symposium on Programming Languages and Software Tools SPLST'03*, Kuopio, Finland, June 17-18, 2003, pp.187-200.

[39] SUCHETA, C., SAIBAL, K. P. and SUGATA, G. An Improved 3-Quasigroup based Encryption Scheme. In: *ICT Innovations 2012, Secure and Intelligent Systems*, Ohrid, Macedonia, Web Proceedings, 2012, pp.173-184. ISSN 1857-7288.

[40] CSORGO, P., SHCHERBACOV, V. *On some quasigroup cryptographical primitives*, 2011, 11 p. [online]. https://arxiv.org/abs/1110.6591

[41] MOLDOVYAN, N.A., SHCHERBACOV, A.V and SHCHERBACOV, V.A. On some applications of quasigroups in cryptology. In: *Proceedings of the Workshop on Foundations of Informatics FOI-2015*, August 24-29, 2015, Chisinau, Republic of Moldova, pp.331-341. ISBN 978-9975-4237-3-1.

[42] ГРИБОВ, А.В. *Алгебраические неассоциативные структуры и их приложения в криптологии*. Кандидатская диссертация, кандидата физико-математических наук, МГУ, Москва, 2015, 93 с.

[43] БЕЛОУСОВ, В.Д. *n-арные квазигруппы*. Кишинев: Штиинца, 1972, 225 с.

[44] ELGAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: *IEEE Transactions on Information Theory*, 1985, Vol.31, No.4, pp. 469-472. ISSN 0018-9448.

[45] SHCHERBACOV, V.A. On the structure of left and right F-, SM- and E-quasigroups. In: *Journal of Generalized Lie Theory and Applications*, 2009, Vol. 3, No.3, pp.197-259. ISSN 1736-5279.

[46] VOJVODA, M. Cryptanalysis of a file encoding system based on quasigroup. In: *Journal of Electrical Engineering*, 2003, Vol.54, No.12. ISSN 1335-3632.

[47] VOJVODA, M. *Attacks on a file encryption system based on quasigroup*. In: *Proceedings of Elitech 2003*, Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology,2003, Bratislava, Slovak Republic, pp. 54-56

ADNOTARE

Maliutina Nadejda: "Utilizarea tehnologiilor informaționale la elaborarea algoritmilor criptografici și algebrici"

Teză de doctor în informatică, Chișinău, 2023

Structura tezei: teza constă din introducere, patru capitole, concluzii generale și recomandări, bibliografie din 201 titluri și 3 anexe. Teza conține 145 pagini de text de bază, o figură și 71 tabele. Rezultatele obținute sunt publicate în 21 lucrări ştiințifice.

Cuvinte-cheie: algoritm Markovski, cvazigrup, cvazigrup de stânga și de dreapta, translație, text deschis, text cifrat, atac, cheie, criptare, decriptare.

Scopul lucrării: construirea noilor și îmbunătățirea algoritmilor criptografici deja construiți și a criptoanalizei acestora.

Obiectivele cercetării: 1. Dezvoltarea unui algoritm criptografic eficient bazat pe algoritmul Markovski folosind grupoizi n-ari; 2. Elaborarea programelor, care implementează lucrul algoritmilor construiti; 3. Efectuarea atacurilor asupra tuturor cifrurilor construite; 4. Analiza comparativă a atacurilor comise; 5. Găsirea textelor de lungime minimă pentru toate tipurile de atacuri investigate.

Noutatea și originalitatea științifică: Rezultatele lucrării sunt noi și originale. Ele sunt o continuare a cercetărilor anterioare în acest domeniu. Au fost dezvoltați și generalizați algoritmi, care au permis îmbunătățirea activității algoritmului clasic Markovski, au fost studiate atacurile asupra cifrurilor construite și a fost arătat gradul de rezistență al acestor cifruri.

Rezultatul obținut care contribuie la soluționarea unei probleme ştiinţifice importante: constă în dezvoltarea noilor generalizări ale algoritmului clasic care cresc rezistența cifrului construit la tipuri cunoscute de atacuri.

Semnificația teoretică a lucrării: este determinată prin obținerea noilor algoritmi și cifrurilor construite, folosind structuri neasociative precum grupoizi n-ari. Sunt dezvoltate noi generalizări ale algoritmilor de codare folosind cvazigrupuri de stânga și de dreapta, grupoizi n-ari inversabili la un loc fixat.

Valoarea aplicativă: constă în utilizarea rezultatelor obținute în teoria codificării și criptoanaliză.

Implementarea rezultatelor ştiinţifice: rezultatele obținute pot fi utilizate în cercetările științifice legate de codificarea datelor, studierea eficienței prezentării informațiilor și criptoanaliza datelor. Ele pot fi utilizate și în proiectarea unui curs opțional pentru studenții universitari legat de studiul criptologiei pe structuri algebrice abstracte.

ANNOTATION

Malyutina Nadezhda: "The use of information technologies in the development of cryptographic and algebraic algorithms"

PhD Thesis in Computer Science, Chisinau, 2023

Thesis structure: the thesis consists of Introduction, four main chapters, general conclusions and recommendations, bibliography of 201 sources, and 3 annexes. The thesis contains 145 pages of the main text, one figure, and 71 tables. The obtained results were published in 21 scientific works.

Keywords: Markovski algorithm, quasigroup, left and right quasigroup, translation, plaintext, ciphertext, attack, key, encryption, decryption.

The purpose of the thesis: construction of new modifications and improvement of already developed cryptographic algorithms and their cryptanalysis.

The objectives of the work: 1. Development of an effective cryptographic algorithm based on the Markovski algorithm using n-ary groupoids; 2. Writing programs that perform the work of the constructed algorithms; 3. Carrying out attacks on all built ciphers; 4. Comparative analysis of the attacks carried out; 5. Finding texts of the minimum length for all investigated types of attacks.

The scientific novelty and originality: the main results of the work are new and original. They are a continuation of previous research in this area. Algorithms were developed and generalized that allowed us improving the work of the classical Markovski algorithm, the attacks on the constructed ciphers were studied, and the degree of resistance of these ciphers was shown.

The important scientific problem being solved in the research: it consists in the development of new generalizations of the classical algorithm, which contribute to an increase in the resistance of the constructed cipher to known types of attacks.

The theoretical significance of the thesis: is determined by obtaining new algorithms and ciphers built using non-associative structures such as n-ary groupoids. New generalizations of coding algorithms using left and right quasigroups, n-ary groupoids invertible in one fixed place are developed.

The applicative value of the thesis: it lies in the use of the obtained results in coding theory and cryptanalysis.

The implementation of the scientific results: the results obtained can be used in scientific research related to data coding, study of the efficiency of information presentation, and data cryptanalysis. They can also be used in the design of an elective course for university students related to the study of cryptology on abstract algebraic structures.

АННОТАЦИЯ

Малютина Надежда: "Использование информационных технологий в разработке криптографических и алгебраических алгоритмов"

Докторская диссертация по информатике, Кишинёв, 2023

Структура диссертации: диссертация и состоит из введения, четырех глав, общих выводов и рекомендаций, списка литературы из 201 источника и 3 приложений. Диссертация содержит 145 страницы основного текста, 1 рисунок и 71 таблицу. Полученные результаты были опубликованы в 21 научных работах.

Ключевые слова: Алгоритм Марковского, квазигруппа, левая и правая квазигруппа, трансляция, открытый текст, зашифрованный текст, атака, ключ, шифрование, дешифрование.

Цель исследования: построение новых и усовершенствование уже построенных криптографических алгоритмов и их криптоанализ.

Задачи исследования: 1. Разработка эффективного криптографического алгоритма на основе алгоритма Марковского с использованием n-арных группоидов; 2. Написание программ, реализующих работу построенных алгоритмов; 3. Проведение атак на все построенные шифры; 4. Сравнительный анализ проведенных атак; 5. Нахождение текстов минимальной длины для всех исследованных типов атак.

Научная новизна и оригинальность работы: результаты работы новые и оригинальные. Они являются продолжением предыдущих исследований в этой области. Разработаны и обобщены алгоритмы, которые позволили улучшить работу классического алгоритма Марковского, изучены атаки на построенные шифры и показана степень стойкости этих шифров.

Полученный результат, который способствует решению важной научной проблемы: состоит в разработке новых обобщений классического алгоритма, которые способствуют увеличению стойкости построенного шифра к известным видам атак.

Теоретическая значимость работы: определяется получением новых алгоритмов и шифров, построенных с применением неассоциативных структур, таких как n-арные группоиды. Разработаны новые обобщения алгоритмов кодирования с использованием левых и правых квазигрупп, n-арных группоидов обратимых на одном фиксированном месте.

Прикладная ценность работы заключается в использовании полученных результатов в теории кодирования и криптоанализе.

Внедрение научных результатов: Полученные результаты могут быть использованы в научных исследованиях, связанных с кодированием данных, изучением эффективности представления информации, криптоанализе данных. Они также могут быть использованы при разработке факультативного курса для студентов университетов, связанного с изучением криптологии на абстрактных алгебраических структурах.

MALIUTINA NADEJDA

UTILIZAREA TEHNOLOGIILOR INFORMAȚIONALE LA ELABORAREA ALGORITMILOR CRIPTOGRAFICI ȘI ALGEBRICI

122.03 – Modelare, metode matematice, produse program

Rezumatul tezei de doctor în informatică

Aprobat spre tipar: 09.03.2023	Formatul hărtiei 60x84 1/16
Hărtie ofset.Tipar ofset.	Tiraj 30 ex.
Coli de tipar.: 1,5	Comanda nr. 15

Mag. "PRINTER", str. Sverdlov, 92, Tiraspol, MD-3300

Email: alex@impreso.md